

Game-theoretic characterization of antidegradable channels

Francesco Buscemi^{*1}, Nilanjana Datta^{†2}, and Sergii Strelchuk^{‡3}

¹Graduate School of Information Science, Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan

²Statistical Laboratory, University of Cambridge, Cambridge CB3 0WB, U.K.

³Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, U.K.

Abstract

We introduce a guessing game involving a quantum channel, three parties—the sender, the receiver and an eavesdropper, Eve—and a quantum public side channel. We prove that a necessary and sufficient condition for the quantum channel to be antidegradable, is that Eve wins the game. We thus obtain a complete operational characterization of antidegradable channels in a game-theoretic framework.

1 Introduction

There are numerous tasks in quantum information theory which involve the use of quantum channels. A quantum channel has many different capacities, depending on the task at hand, the nature of the information transmitted, and available resources. For example, the quantum capacity of a channel quantifies its potential for communication of quantum information, whereas its private capacity quantifies its potential for secure communication of classical information [1]. Deciding whether a given quantum channel has a positive capacity is a non-trivial problem, e.g. there does not exist a unique criterion to determine whether the quantum capacity of a given channel is zero. Classical channels with zero capacity are uninteresting in the information-theoretic sense. In contrast, quantum channels with zero capacity exhibit intriguing behavior as shown by the superactivation phenomenon [12]: there exist examples of pairs of channels with zero quantum capacity, which, when used in tandem, allow transmission of quantum information. One particular class of zero-capacity channels consists of *antidegradable channels*. For such a channel, a post-processing of its environment can simulate the output of the channel [2]. The no-cloning theorem [5] ensures that such channels have zero quantum capacity. The simplest example of the latter is a 50% erasure channel which with equal probability either transmits the input state perfectly or replaces it with an erasure flag. However, there are other non-trivial examples of channels with zero quantum capacity, e.g., the positive partial transpose (PPT) channels [6]. In addition, antidegradable channels also have zero private capacity (unlike PPT channels), but whether they are the only non-trivial quantum channels with this property is an open question (since there exist echo-correctable channels with arbitrarily small, but non-zero, private capacity [8, 7]). Therefore, the knowledge that a given channel has zero quantum and private capacity is not sufficient to conclude that it is antidegradable. This leads us to the following question:

(Q): Is there a setting in which one can obtain a complete operational characterization of antidegradable channels?

In this paper we answer this question in the affirmative by constructing a game-theoretic framework which involves the noisy quantum channel \mathcal{N} (which we wish to characterize), a quantum public side channel \mathcal{S} , and three parties: Alice (the sender), Bob (the receiver) and Eve (the eavesdropper). Alice sends classical information to Bob through \mathcal{N} , whose environment is accessible to Eve. Alice also sends information through \mathcal{S} , which is accessible to both Bob and Eve.

^{*}buscemi@is.nagoya-u.ac.jp

[†]n.datta@statslab.cam.ac.uk

[‡]ss870@cam.ac.uk

The game is constructed as follows (formal definitions are given in Section 2).

1.1 The guessing game

1. Alice chooses a letter x at random from a given finite alphabet \mathcal{X} , and encodes it in a bipartite state, say $\rho_{AA_0}^x$.
2. The A part of the input is sent through \mathcal{N} , while the A_0 part is transmitted via \mathcal{S} .
3. Bob then obtains the output of \mathcal{N} while Eve receives the information that is transmitted to the channel's environment. In other words, she receives the output of the *complementary channel* \mathcal{N}_{env} (see Section 2 for its definition). In addition, they both receive the output of \mathcal{S} .
4. The task now, for both Bob and Eve, is to guess which letter x Alice chose. Since Bob and Eve are competing, they both adopt the optimal guessing strategy they have available. Correspondingly, the reliabilities of their guesses is measured by the optimal guessing probabilities of the ensembles of states they receive.
5. Bob wins the game whenever his guessing probability is *strictly higher* than that of Eve (i.e. in the case of a draw, Eve wins).

The situation is depicted in Figure 1 below.

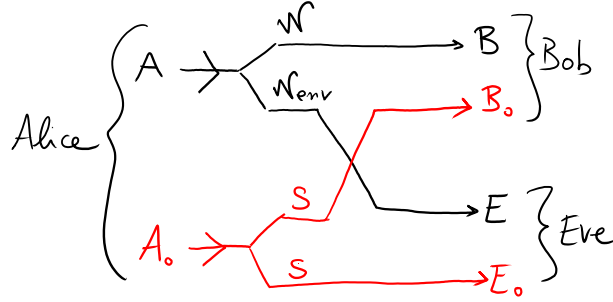


Figure 1: Structure of the guessing game: Alice communicates with Bob using the quantum channel \mathcal{N} (i.e. the one which we want to characterize) and a quantum channel \mathcal{S} , which is public, in the sense that it conveys the same output to Bob and Eve. A natural example of such a public channel is a symmetric channel [21, 22, 23]. Bob plays the guessing game against Eve, who has access to the environment of \mathcal{N} (labelled by \mathcal{N}_{env}) and \mathcal{S} .

To state our main result (Theorem 1) which leads to the characterization of antidegradable channels, we first introduce the notion of *extension* of a quantum channel: for any pair of quantum channels $(\mathcal{N}_\alpha, \mathcal{N}_\beta)$ we say that \mathcal{N}_α is an *extension* of \mathcal{N}_β if $\mathcal{N}_\beta = \mathcal{D} \circ \mathcal{N}_\alpha$ for some quantum channel \mathcal{D} . This is a generalization of the notion of *degradable extension* of the channel (introduced in [25]) which corresponds to the case in which the channel \mathcal{N}_α is degradable and \mathcal{N}_β is complementary to it. Then our result can be stated as follows: for any given input ensemble of states, the guessing probability of the output ensemble of \mathcal{N}_α is higher than that of \mathcal{N}_β , if and only if \mathcal{N}_α is an extension of \mathcal{N}_β . We establish the above result by first proving its analogue for statistical comparison of bipartite states and then using Choi isomorphism.

Consider the case in which \mathcal{N}_β is the quantum channel \mathcal{N} employed in the guessing game 1.1, and \mathcal{N}_α is the channel \mathcal{N}_{env} which is complementary to it. For this choice, our result (Theorem 1) implies that \mathcal{N} is antidegradable *if and only if* Eve always wins, regardless of the choice of Alice's encoding strategy. In other words, our result shows that, *for any* channel which is not antidegradable, there exists (at least) one encoding strategy which Alice can choose to make Bob win the guessing game.

We note that even though the scenario of our guessing game is 'cryptographic' in its nature (since Bob and Eve compete), proving that Bob is able to win against Eve in the guessing game is insufficient

to conclude that any *information-theoretic secrecy* can be established between Alice and Bob. This is because, in the guessing game, we only compare the guessing probabilities of Bob and Eve, and not the mutual informations between the random variables corresponding to their respective inferences and that of the random variable corresponding to Alice's input. However, the game-theoretic scenario 1.1 has the particular advantage of singling out antidegradable channels as the only channels for which Eve necessarily wins. In other words, a *necessary and sufficient condition* for the quantum channel \mathcal{N} to be antidegradable is that Eve wins the guessing game, for any possible encoding strategy Alice may choose.

The paper is organized as follows. In Section 2 we introduce the necessary notation and definitions, and then state our main result (Theorem 1). In Section 3 we derive an analogue of Theorem 1 for partial orderings of bipartite quantum states. In Section 4 we use this result, in conjunction with the Choi isomorphism, to obtain a proof of Theorem 1. Some further implications of Theorem 1 for convex combinations of channels and their extensions are given in 5. We end with a brief summary and open questions in Section 6.

2 Main result

2.1 Notation and definitions

In what follows, we only consider quantum systems defined on finite dimensional Hilbert spaces \mathcal{H} . We denote by $\mathbf{L}(\mathcal{H})$ the set of all linear operators acting on \mathcal{H} , and by $\mathbf{S}(\mathcal{H})$ the set of all density operators (or *states*) $\rho \in \mathbf{L}(\mathcal{H})$, with $\rho \geq 0$ and $\text{Tr}[\rho] = 1$. The identity operator in $\mathbf{L}(\mathcal{H})$ will be denoted by the symbol $\mathbb{1}$, whereas the identity map from $\mathbf{L}(\mathcal{H})$ to itself will be denoted by id . A *positive-operator valued measure* (POVM) is a family $\mathbb{P} = \{P^x\}_{x \in \mathcal{X}} \subset \mathbf{L}(\mathcal{H})$ of operators $P^x \geq 0$, labelled by a finite index set $\mathcal{X} = \{x\}$ (i.e. the *outcome set*), such that $\sum_{x \in \mathcal{X}} P^x = \mathbb{1}$.

In what follows, a *channel* is considered as a triple $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$, where \mathcal{H}_A is the input Hilbert space, \mathcal{H}_B is the output Hilbert space, and $\mathcal{N} : \mathbf{L}(\mathcal{H}_A) \rightarrow \mathbf{L}(\mathcal{H}_B)$ is a completely positive, trace-preserving (CPTP) linear map. Where possible, we will denote a channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ simply as \mathcal{N} . The adjoint (Heisenberg dual) of a linear map $\mathcal{N} : \mathbf{L}(\mathcal{H}_A) \rightarrow \mathbf{L}(\mathcal{H}_B)$ is the linear map $\mathcal{N}^* : \mathbf{L}(\mathcal{H}_B) \rightarrow \mathbf{L}(\mathcal{H}_A)$ defined with respect to the Hilbert-Schmidt inner product by $\text{Tr}[\mathcal{N}^*(X) Y] := \text{Tr}[X \mathcal{N}(Y)]$, for all $X \in \mathbf{L}(\mathcal{H}_B)$ and $Y \in \mathbf{L}(\mathcal{H}_A)$. Therefore, if \mathcal{N} is a channel, its adjoint \mathcal{N}^* is a completely positive, unital (unit-preserving), i.e. $\mathcal{N}^*(\mathbb{1}_B) = \mathbb{1}_A$, linear map (and vice versa).

Given a channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$, its *Stinespring isometric dilation* [13] is given by a complementary (ancillary) quantum system \mathcal{H}_E (the 'environment') together with an isometry $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$, $V^\dagger V = \mathbb{1}_A$, such that

$$\mathcal{N}(X) = \text{Tr}_E[V X V^\dagger], \quad \forall X \in \mathbf{L}(\mathcal{H}_A).$$

The Stinespring isometric dilation, which always exists, can be considered to be essentially unique, in the sense that it is unique up to isometric equivalences on \mathcal{H}_E . This leads us to define an essentially unique complementary channel $(\mathcal{H}_A, \mathcal{H}_E, \mathcal{N}_{\text{env}})$ as follows [3, 14]:

$$\mathcal{N}_{\text{env}}(Y) := \text{Tr}_B[V Y V^\dagger].$$

Definition 1 (Antidegradable channels). *Given a channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$, let $(\mathcal{H}_A, \mathcal{H}_E, \mathcal{N}_{\text{env}})$ be its complementary channel. \mathcal{N} is called antidegradable if and only if there exists another channel $(\mathcal{H}_E, \mathcal{H}_B, \mathcal{D})$ such that*

$$\mathcal{N} = \mathcal{D} \circ \mathcal{N}_{\text{env}}.$$

(It is easy to verify that the property of being antidegradable does not depend on the particular Stinespring isometric dilation chosen to construct the complementary channel.)

In other words, an eavesdropper, Eve, who has access to the environment of an antidegradable channel, can perfectly simulate the output of the channel by means of a fixed post-processing which is independent of the input. In this sense, Eve always receives *more information* than the receiver Bob. As a straightforward consequence, antidegradable channels turn out to have zero capacity for any information-theoretic protocol that aims to put Bob in a position of advantage over eavesdropper.

Another notion we need is the following [21]:

Definition 2 (d -dimensional symmetric channels). For a given finite integer $d \geq 2$, let \mathcal{H}_A be a $\frac{d(d+1)}{2}$ -dimensional Hilbert space, \mathcal{H}_B and \mathcal{H}_E be d -dimensional Hilbert spaces; moreover, let $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$ be any isometry embedding \mathcal{H}_A into the symmetric subspace $(\mathcal{H}_B \otimes \mathcal{H}_E)_{\text{sym}}$; the channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{S})$, defined by its action $\mathcal{S}(\rho) := \text{Tr}_E[V \rho V^\dagger]$ for all $\rho \in \mathbf{S}(\mathcal{H}_A)$, is called a d -dimensional symmetric channel.

It should be clear then that d -dimensional symmetric channels are, in particular, antidegradable, with the post-processing channel \mathcal{D} given by the identity map. The class of symmetric quantum channels has been identified as the quantum analogue of a *public channel* [21, 22, 23], since, for a symmetric channel, the receiver and eavesdropper receive the same output [24].

2.2 Statement of the main result

Before stating our main result we introduce some further definitions.

Definition 3. A (finite) ensemble of quantum states \mathfrak{m} is defined as a triple $(\mathcal{H}, \mathcal{X}, \mathcal{E})$, where \mathcal{H} is a finite-dimensional input Hilbert space, $\mathcal{X} = \{x\}$ is a finite indexing alphabet, and $\mathcal{E} = \{p_x, \rho_x^x\}_{x \in \mathcal{X}}$ is a collection of quantum states $\rho_x^x \in \mathbf{S}(\mathcal{H})$ and probabilities p_x .

Consider now a quantum channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ and an ensemble $\mathfrak{m} = (\mathcal{H}_A, \mathcal{X}, \mathcal{E})$. We can then imagine the situation in which a sender (say, Alice) chooses a letter $x \in \mathcal{X}$ at random according to the probability distribution p_x , prepares a quantum system in the corresponding state ρ_A^x , and sends this through \mathcal{N} to a receiver (say, Bob), who has to guess the input letter chosen by Alice. This setup can be formally described as follows:

Definition 4 (Dynamical guessing games). Let $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ be a quantum channel, $(\mathcal{H}_A, \mathcal{X}, \mathcal{E})$ an ensemble. The corresponding guessing game is defined as the task of correctly guessing letter x upon receiving $\mathcal{N}(\rho_A^x)$. The optimal probability of winning the game is given by

$$p^*(\mathcal{N}, \mathfrak{m}) := \max_{\mathbb{P}_B} \sum_{x \in \mathcal{X}} p_x \text{Tr}[P_B^x \mathcal{N}(\rho_A^x)]. \quad (1)$$

Equation (1) above measures ‘how good’ is a given channel \mathcal{N} for communicating the information about \mathcal{X} encoded in \mathfrak{m} . Accordingly, given another channel $(\mathcal{H}_A, \mathcal{H}_{B'}, \mathcal{M})$, with same input space but generally different output space, one can say that ‘ \mathcal{N} is not worse than \mathcal{M} with respect to \mathfrak{m} ’ if $p^*(\mathcal{N}, \mathfrak{m}) \geq p^*(\mathcal{M}, \mathfrak{m})$. By extending this definition to every possible finite ensemble, we obtain the following partial ordering relation between quantum channels:

Definition 5. Given two quantum channels with the same input space $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_\alpha)$ and $(\mathcal{H}_A, \mathcal{H}_{B'}, \mathcal{N}_\beta)$, we say that ‘ \mathcal{N}_α is more informative than \mathcal{N}_β ,’ and denote it as $\mathcal{N}_\alpha \supseteq \mathcal{N}_\beta$, whenever $p^*(\mathcal{N}_\alpha, \mathfrak{m}) \geq p^*(\mathcal{N}_\beta, \mathfrak{m})$, for all finite ensembles \mathfrak{m} on \mathcal{H}_A .

Clearly, guessing games can be also played with more than one channel arranged ‘in parallel,’ as follows. Consider for example two quantum channels $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ and $(\mathcal{H}_{A_0}, \mathcal{H}_{B_0}, \mathcal{M})$ and an ensemble defined on the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_{A_0}$, i.e. $\mathfrak{n} = (\mathcal{H}_A \otimes \mathcal{H}_{A_0}, \mathcal{X}, \mathcal{E})$. Then, in analogy with (1), we have

$$p^*(\mathcal{N} \otimes \mathcal{M}, \mathfrak{n}) = \max_{\mathbb{P}_{BB_0}} \sum_{x \in \mathcal{X}} p_x \text{Tr}[P_{BB_0}^x (\mathcal{N} \otimes \mathcal{M})(\rho_{AA_0}^x)]. \quad (2)$$

It is important to stress that, as the input states $\rho_{AA_0}^x$ can be entangled, so the elements $P_{BB_0}^x$ of the decoding POVM are allowed to act globally on the output. By means of parallelized guessing games, a stronger partial ordering relation can be introduced as follows:

Definition 6 (Strong information ordering). Given two quantum channels with the same input space $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_\alpha)$ and $(\mathcal{H}_A, \mathcal{H}_{B'}, \mathcal{N}_\beta)$, we say that ‘ \mathcal{N}_α is strongly more informative than \mathcal{N}_β ,’ and denote it as

$$\mathcal{N}_\alpha \supseteq_s \mathcal{N}_\beta,$$

whenever $\mathcal{N}_\alpha \otimes \mathcal{M} \supseteq \mathcal{N}_\beta \otimes \mathcal{M}$, for all quantum side channels $(\mathcal{H}_{A_0}, \mathcal{H}_{B_0}, \mathcal{M})$.

In the above definition, we allow the comparison between \mathcal{N}_α and \mathcal{N}_β to be made in parallel with any possible quantum side channel $(\mathcal{H}_{A_0}, \mathcal{H}_{B_0}, \mathcal{M})$ considered as an auxiliary communication resource. It is often interesting, however, to constrain the side channel to belong to some restricted class of channels, typically with reduced communication capability. As a trivial example, Definition 5 can be considered as a special case of Definition 6, in which side channels are restricted to those which map all input states to the same output state. Here, for reasons that will be clarified later, we are in particular interested in the case in which the quantum side channel is a symmetric channel $(\mathcal{H}_{A_0}, \mathcal{H}_{B_0}, \mathcal{S})$, as introduced in Definition 1:

Definition 7 (Weak information ordering). *Given two quantum channels with the same input space $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_\alpha)$ and $(\mathcal{H}_A, \mathcal{H}_{B'}, \mathcal{N}_\beta)$, we write*

$$\mathcal{N}_\alpha \supseteq_w \mathcal{N}_\beta,$$

whenever there exists a symmetric quantum side channels $(\mathcal{H}_{A_0}, \mathcal{H}_{B_0}, \mathcal{S})$, with $\mathcal{H}_{B_0} \cong \mathcal{H}_{B'}$, such that $\mathcal{N}_\alpha \otimes \mathcal{S} \supseteq \mathcal{N}_\beta \otimes \mathcal{S}$.

Notice that the above definition relaxes Definition 6, not only in that the comparison can be made just with respect to symmetric side channels (rather than *any* side channel), but just with respect to *some* symmetric side-channel (under the sole condition $\mathcal{H}_{B_0} \cong \mathcal{H}_{B'}$).

The main technical result of this paper is summarised in the following theorem, for which a proof will be given in Section 4:

Theorem 1. *Let $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_\alpha)$ and $(\mathcal{H}_A, \mathcal{H}_{B'}, \mathcal{N}_\beta)$ be two quantum channels with the same input space \mathcal{H}_A . Then, the following are equivalent:*

1. *there exists a third quantum channel $(\mathcal{H}_B, \mathcal{H}_{B'}, \mathcal{D})$ such that $\mathcal{N}_\beta = \mathcal{D} \circ \mathcal{N}_\alpha$;*
2. *$\mathcal{N}_\alpha \supseteq_s \mathcal{N}_\beta$;*
3. *$\mathcal{N}_\alpha \supseteq_w \mathcal{N}_\beta$.*

An interesting interpretation of Theorem 1 is obtained when \mathcal{N}_β and \mathcal{N}_α are taken to be the channel \mathcal{N} (which we wish to characterize) and its corresponding complementary channel \mathcal{N}_{env} , respectively. In this situation, consider the game-theoretic scenario 1.1 described in the Introduction, in which, at each turn of the game (corresponding to each use of the channel), Bob and Eve are asked to guess the input chosen by Alice. In this case, it is natural to require the side-channel \mathcal{S} to be symmetric, so that it serves as a public channel [21, 22, 23], since it conveys the same information to Bob and Eve.

Theorem 1 then implies the following corollary which provides a complete characterization of antidegradable channels in the game-theoretic scenario 1.1:

Corollary 1. *A channel is not antidegradable if and only if there exists an encoding strategy for Alice which results in Bob winning the game 1.1.*

The above corollary guarantees that any channel \mathcal{N} , as long as it is not antidegradable, puts Bob in a position of advantage with respect to Eve in the game 1.1.

3 From quantum channels to bipartite states...

In this section we derive results pertaining to quantum states, which are analogues of the results stated in Theorem 1 for quantum channels. We begin by recalling a fundamental relation, due to Choi [17], between bipartite states and channels.

Theorem 2 (Choi Isomorphism). *Fix an orthonormal basis $\{|i\rangle\}_{i=1}^d$ in a finite-dimensional Hilbert space \mathcal{H}_A ($\dim \mathcal{H}_A = d$). Define the standard maximally entangled state $|\Phi^+\rangle := d^{-1/2} \sum_{i=1}^d |i\rangle \otimes |i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_A$. Then, any channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ defines a bipartite state $\rho_{AB}^\mathcal{N} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ with $\text{Tr}_B[\rho_{AB}^\mathcal{N}] = d^{-1} \mathbb{1}_A$ via the relation:*

$$\rho_{AB}^\mathcal{N} := (\text{id} \otimes \mathcal{N})(|\Phi^+\rangle\langle\Phi^+|).$$

Conversely, any bipartite state $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ with $\text{Tr}_B[\rho_{AB}] = d^{-1} \mathbb{1}_A$ defines a channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}^\rho)$ via the relation:

$$\mathcal{N}^\rho(X) := d \text{Tr}_A[(X^T \otimes \mathbb{1}_B) \rho_{AB}],$$

for all $X \in \mathbf{L}(\mathcal{H}_A)$, where the transposition is taken with respect to the fixed basis $\{|i\rangle\}_{i=1}^d$. The correspondence is one-to-one, i.e.

$$d \text{Tr}_A[(X^T \otimes \mathbb{1}_B) \rho_{AB}^\mathcal{N}] = \mathcal{N}(X),$$

and

$$(\text{id} \otimes \mathcal{N}^\rho)(|\Phi^+\rangle\langle\Phi^+|) = \rho_{AB}.$$

With the Choi isomorphism at hand, we will reformulate Theorem 1 as a result about the comparison of quantum bipartite states, rather than channels, in the spirit of Ref. [19].

3.1 Statistical comparison of bipartite quantum states

As in Ref. [15, 16, 19], we can characterize bipartite quantum states in terms of the following game-theoretical scenarios:

- **Quantum Statistical Decision Games:** these are defined by an outcome set $\mathcal{X} = \{x\}$ and a family of self-adjoint operators $\{O_A^x\}_{x \in \mathcal{X}}$; given a bipartite quantum state $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, its payoff with respect to a quantum statistical decision game is given by

$$\max_{\mathbf{Q}_B} \sum_x \text{Tr}[(O_A^x \otimes Q_B^x) \rho_{AB}]. \quad (3)$$

- **Quantum Statistical Decision Problems:** these are defined by two outcome sets $\mathcal{X} = \{x\}$ and $\mathcal{Y} = \{y\}$, a POVM $\{P_A^x\}_{x \in \mathcal{X}}$, and a utility function $u : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}$; given a bipartite quantum state $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, its payoff with respect to a quantum statistical decision problem is given by

$$\max_{\mathbf{Q}_B} \sum_{x,y} u(x,y) \text{Tr}[(P_A^x \otimes Q_B^y) \rho_{AB}]. \quad (4)$$

- **Static Guessing Games:** these are defined by an outcome set $\mathcal{X} = \{x\}$ and a POVM $\{P_A^x\}_{x \in \mathcal{X}}$; given a bipartite quantum state $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, its payoff with respect to a guessing game is given by

$$\max_{\mathbf{Q}_B} \sum_x \text{Tr}[(P_A^x \otimes Q_B^x) \rho_{AB}]. \quad (5)$$

As done in Definition 5, where quantum channels are compared with respect to their ‘utility’ in playing guessing games, we can compare bipartite states in terms of their ‘utilities’ in playing the three kinds of statistical games we introduced above. The following theorem states that, in the case in which we are to compare two bipartite states $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_{AB'} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_{B'})$, such that $\text{Tr}_B \rho_{AB} = \text{Tr}_{B'} \sigma_{AB'}$, the corresponding partial ordering relations are all equivalent.

Theorem 3. *Let $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_{AB'} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_{B'})$ be such that $\text{Tr}_B \rho_{AB} = \text{Tr}_{B'} \sigma_{AB'}$. Then, the following statements are equivalent:*

1. *Comparison by quantum statistical decision games. For any outcome set $\mathcal{X} = \{x\}$ and for any set of self-adjoint operators $\{O_A^x\}_{x \in \mathcal{X}}$,*

$$\max_{\mathbf{R}_B} \sum_x \text{Tr}[(O_A^x \otimes R_B^x) \rho_{AB}] \geq \max_{\mathbf{Q}_{B'}} \sum_x \text{Tr}[(O_A^x \otimes Q_{B'}^x) \sigma_{AB'}]; \quad (6)$$

2. *Comparison by quantum statistical decision problems. For any outcome sets $\mathcal{X} = \{x\}$ and $\mathcal{Y} = \{y\}$, for any POVM $\{P_A^x\}_{x \in \mathcal{X}}$, and for any utility function $u : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}$,*

$$\max_{\mathbf{R}_B} \sum_{x,y} u(x,y) \text{Tr}[(P_A^x \otimes R_B^y) \rho_{AB}] \geq \max_{\mathbf{Q}_{B'}} \sum_{x,y} u(x,y) \text{Tr}[(P_A^x \otimes Q_{B'}^y) \sigma_{AB'}]; \quad (7)$$

3. *Comparison by the Hahn-Banach separation theorem.* For any outcome sets $\mathcal{X} = \{x\}$ and $\mathcal{Y} = \{y\}$, for any POVMs $\{P_A^x\}_{x \in \mathcal{X}}$ and $\{Q_{B'}^y\}_{y \in \mathcal{Y}}$, there exists a POVM $\{R_B^y\}_{y \in \mathcal{Y}}$ such that

$$\text{Tr}[(P_A^x \otimes R_B^y) \rho_{AB}] = \text{Tr}[(P_A^x \otimes Q_{B'}^y) \sigma_{AB'}] \quad \forall x, y; \quad (8)$$

4. *Comparison by guessing games.* For any outcome set $\mathcal{X} = \{x\}$ and for any POVM $\{P_A^x\}_{x \in \mathcal{X}}$,

$$\max_{\mathbb{R}_B} \sum_x \text{Tr}[(P_A^x \otimes R_B^x) \rho_{AB}] \geq \max_{\mathbb{Q}_{B'}} \sum_x \text{Tr}[(P_A^x \otimes Q_{B'}^x) \sigma_{AB'}]. \quad (9)$$

Proof. The relation (1) \Rightarrow (2) holds because any specification of an outcome set \mathcal{X} together with a utility function u defines, in particular, a set of self-adjoint operators $\{O_A^y\}_{y \in \mathcal{Y}}$, by the summation $O_A^y := \sum_x u(x, y) P_A^x$. Hence,

$$\begin{aligned} \text{RHS of (7)} &= \max_{\mathbb{Q}_{B'}} \sum_y \text{Tr}[(\sum_x u(x, y) P_A^x) \otimes Q_{B'}^y) \sigma_{AB'}] \\ &= \max_{\mathbb{Q}_{B'}} \sum_y \text{Tr}[(O_A^y \otimes Q_{B'}^y) \sigma_{AB'}] \\ &\leq \max_{\mathbb{R}_B} \sum_y \text{Tr}[(O_A^y \otimes R_B^y) \rho_{AB}] \\ &= \max_{\mathbb{R}_B} \sum_{x, y} u(x, y) \text{Tr}[(P_A^x \otimes R_B^y) \rho_{AB}] \\ &= \text{LHS of (7)}, \end{aligned} \quad (10)$$

where the inequality follows from (1) and the third equality follows from the definition of O_A^y .

The relation (2) \Leftrightarrow (3) holds as a consequence of the separation theorem for convex sets (for a detailed discussion on this point see, for example, Ref. [19]).

The relation (2) \Rightarrow (4) holds simply by taking $u(x, y) = \delta_{xy}$ in (7).

The relation (4) \Rightarrow (1) (which would complete the proof of equivalence) can be established as follows: Given an outcome set \mathcal{X} and a set of self-adjoint operators $\{O_A^x\}_{x \in \mathcal{X}}$, let us define the following operators for $x \in \mathcal{X}$:

$$P_A^x := \frac{1}{\lambda} \frac{1}{|\mathcal{X}|} \left\{ O_A^x + \lambda \mathbb{1}_A - \frac{1}{|\mathcal{X}|} \Sigma_A \right\},$$

where $\Sigma_A := \sum_x O_A^x$ and $0 < \lambda < \infty$ is chosen such that $P_A^x \geq 0$ for all x . By construction $\sum_x P_A^x = \mathbb{1}_A$, and hence $\{P_A^x\}_{x \in \mathcal{X}}$ is a POVM. For each $x \in \mathcal{X}$, then,

$$O_A^x = \lambda |\mathcal{X}| P_A^x - \lambda \mathbb{1}_A + \frac{1}{|\mathcal{X}|} \Sigma_A. \quad (11)$$

Substituting (11) on the RHS of (6) we get

$$\begin{aligned} \text{RHS of (6)} &= \max_{\mathbb{Q}_{B'}} \sum_x \text{Tr} \left\{ \left[\left(\lambda |\mathcal{X}| P_A^x - \lambda \mathbb{1}_A + \frac{1}{|\mathcal{X}|} \Sigma_A \right) \otimes Q_{B'}^x \right] \sigma_{AB'} \right\} \\ &= \lambda |\mathcal{X}| \max_{\mathbb{Q}_{B'}} \left\{ \sum_x \text{Tr}[(P_A^x \otimes Q_{B'}^x) \sigma_{AB'}] \right\} - \lambda + \frac{1}{|\mathcal{X}|} \text{Tr} \Sigma_A \rho_A, \\ &\leq \lambda |\mathcal{X}| \max_{\mathbb{R}_B} \left\{ \sum_x \text{Tr}[(P_A^x \otimes R_B^x) \rho_{AB}] \right\} - \lambda + \frac{1}{|\mathcal{X}|} \text{Tr} \Sigma_A \rho_A \\ &= \max_{\mathbb{R}_B} \sum_x \text{Tr} \left\{ \left[\left(\lambda |\mathcal{X}| P_A^x - \lambda \mathbb{1}_A + \frac{1}{|\mathcal{X}|} \Sigma_A \right) \otimes R_B^x \right] \rho_{AB} \right\} \\ &= \max_{\mathbb{R}_B} \sum_x \text{Tr}[(O_A^x \otimes R_B^x) \rho_{AB}] \\ &= \text{LHS of (6)}, \end{aligned} \quad (12)$$

where the second equality follows from the facts that $\sum_x Q_{B'}^x = \mathbb{1}_{B'}$ and $\text{Tr}_{B'} \sigma_{AB'} = \text{Tr}_B \rho_{AB} \equiv \rho_A$, the inequality follows from (9), and (12) follows from (11). \blacksquare

Remark 1. The condition $\text{Tr}_B \rho_{AB} = \text{Tr}_{B'} \sigma_{AB'}$ is crucial for the validity of Theorem 3. If this condition is dropped, statements (1), (2), and (3) are still equivalent, while statement (4) becomes only a *necessary condition* for the validity of the previous three [19].

We can then introduce the following definition:

Definition 8. Let $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_{AB'} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_{B'})$ be such that $\text{Tr}_B \rho_{AB} = \text{Tr}_{B'} \sigma_{AB'}$. We say that ρ_{AB} is more informative than $\sigma_{AB'}$, written as

$$\rho_{AB} \supseteq_A \sigma_{AB'},$$

if and only if any one of the four statements in Theorem 3 holds.

Finally, as channels can be arranged in parallel and used to play parallelized guessing games (see Definitions 6 and 7), bipartite states too can be put in parallel and compared in a similar manner. For example, given two quantum states $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_{AB'} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_{B'})$ such that $\text{Tr}_B \rho_{AB} = \text{Tr}_{B'} \sigma_{AB'}$, let $\omega_{A_0 B_0} \in \mathbf{S}(\mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0})$ be a third auxiliary bipartite state. Then we can write

$$\rho_{AB} \otimes \omega_{A_0 B_0} \supseteq_{AA_0} \sigma_{AB'} \otimes \omega_{A_0 B_0},$$

with the meaning that for any outcome set $\mathcal{X} = \{x\}$ and for any POVM $\{P_{AA_0}^x\}_x$,

$$\max_{\mathbb{R}_{BB_0}} \sum_x \text{Tr}[(P_{AA_0}^x \otimes R_{BB_0}^x) (\rho_{AB} \otimes \omega_{A_0 B_0})] \geq \max_{\mathbb{Q}_{B'B_0}} \sum_x \text{Tr}[(P_{AA_0}^x \otimes Q_{B'B_0}^x) (\sigma_{AB'} \otimes \omega_{A_0 B_0})].$$

The above equation directly generalizes Eq. (9) in Theorem 3. Along the same line, Eqs. (6), (7), and (8) can also be generalized.

3.2 Local degradability of bipartite states

Another partial ordering relation between bipartite states can be introduced as follows:

Definition 9 (Local degradability). Given two quantum states ρ_{AB} and $\sigma_{AB'}$ such that $\text{Tr}_B \rho_{AB} = \text{Tr}_{B'} \sigma_{AB'}$, we say that ρ_{AB} can be locally degraded to $\sigma_{AB'}$, written as

$$\rho_{AB} \succ \sigma_{AB'}, \quad (13)$$

if and only if there exists a channel $(\mathcal{H}_B, \mathcal{H}_{B'}, \mathcal{D})$ such that

$$\sigma_{AB'} = (\text{id}_A \otimes \mathcal{D}_B)(\rho_{AB}). \quad (14)$$

In Ref. [19], a fundamental equivalence relation between the two orderings \supseteq and \succ is proved. In what follows, we introduce all the ideas we need in order to adapt the equivalence relation of [19] to the present case.

Definition 10 (Local state space and complete states [18, 19]). Given a bipartite state $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, its local state space $\mathbf{S}_B(\rho_{AB}) \subseteq \mathbf{S}(\mathcal{H}_B)$ is the convex set defined as follows:

$$\mathbf{S}_B(\rho_{AB}) = \mathbf{S}(\mathcal{H}_B) \cap \{\text{Tr}_A[(P_A \otimes \mathbb{1}_B) \rho_{AB}] \mid 0 \leq P_A \in \mathbf{L}(\mathcal{H}_A)\}.$$

Whenever $\mathbf{S}_B(\rho_{AB})$ contains $(\dim \mathcal{H}_B)^2$ linearly independent elements, then ρ_{AB} is said to be *B-complete* (or, simply, complete).

Examples of complete bipartite states in $\mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ are given by states of the form $p|\Phi_{AB}^+\rangle\langle\Phi_{AB}^+| + \frac{(1-p)}{d_A d_B} \mathbb{1}_{AB}$, where $|\Phi_{AB}^+\rangle$ is a maximally entangled state in $\mathcal{H}_A \otimes \mathcal{H}_B$, for any $0 < p \leq 1$. We now prove a fact that will turn out to be useful later on:

Lemma 1. A bipartite state $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is *B-complete* if and only if there exists a POVM $\{P_A^x\}_x$ on \mathcal{H}_A such that the set $\{\rho_B^x\}_x$, where $\rho_B^x := \text{Tr}_A[(P_A^x \otimes \mathbb{1}_B) \rho_{AB}]$, contains $(\dim \mathcal{H}_B)^2$ linearly independent elements.

Proof. Suppose that there exists a POVM $\{P_A^x\}_x$ on \mathcal{H}_A such that the set $\{\rho_B^x\}_x$, where $\rho_B^x := \text{Tr}_A[(P_A^x \otimes \mathbb{1}_B) \rho_{AB}]$, contains $(\dim \mathcal{H}_B)^2$ linearly independent elements. Then, define positive operators as follows:

$$\tilde{P}_A^x := \frac{P_A^x}{\text{Tr}[\rho_B^x]},$$

and, correspondingly, $\tilde{\rho}_B^x := \text{Tr}_A[(\tilde{P}_A^x \otimes \mathbb{1}_B) \rho_{AB}]$. Clearly, all $\tilde{\rho}_B^x$ belong to $\mathbf{S}_B(\rho_{AB})$, and they are linearly independent if and only if the ρ_B^x are. Therefore $\mathbf{S}_B(\rho_{AB})$ contains $(\dim \mathcal{H}_B)^2$ linearly independent elements, i.e. ρ_{AB} is B -complete.

Conversely, suppose that ρ_{AB} is B -complete. Then, there exist $(\dim \mathcal{H}_B)^2$ positive operators P_A^x such that all $\rho_B^x = \text{Tr}_A[(P_A^x \otimes \mathbb{1}_B) \rho_{AB}] \in \mathbf{S}_B(\rho_{AB})$ are linearly independent. However, $\sum_x P_A^x \neq \mathbb{1}_A$, i.e. the operators $\{P_A^x\}_x$, even though positive, do not constitute, in general, a POVM. Let then λ be any strictly positive number such that $\lambda \sum_x P_A^x \leq \mathbb{1}_A$, and define $\tilde{P}_A^x := \lambda P_A^x$, and $\tilde{P}_A^\infty := \mathbb{1}_A - \sum_x \tilde{P}_A^x$. Then, the set $\{\tilde{P}_A^x\}_x \cup \{\tilde{P}_A^\infty\}$ constitutes a well defined POVM. Define also $\tilde{\rho}_B^x := \text{Tr}_A[(\tilde{P}_A^x \otimes \mathbb{1}_B) \rho_{AB}]$. Since the first $(\dim \mathcal{H}_B)^2$ elements of $\{\tilde{\rho}_B^x\}$ are linearly independent if and only if the ρ_B^x are, we have that the set $\{\tilde{\rho}_B^x\}$ surely contains $(\dim \mathcal{H}_B)^2$ linearly independent elements. \blacksquare

Theorem 4 (Comparison of bipartite quantum states [19, 20]). *Given two bipartite quantum states $\rho_{AB} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_{AB'} \in \mathbf{S}(\mathcal{H}_A \otimes \mathcal{H}_{B'})$ with $\text{Tr}_B \rho_{AB} = \text{Tr}_{B'} \sigma_{AB'}$, the following are equivalent:*

1. $\rho_{AB} \succ \sigma_{AB'}$;
2. for any \mathcal{H}_{A_0} , any \mathcal{H}_{B_0} , and any auxiliary bipartite state $\omega_{A_0 B_0} \in \mathbf{S}(\mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0})$,
 $\rho_{AB} \otimes \omega_{A_0 B_0} \supseteq_{AA_0} \sigma_{AB'} \otimes \omega_{A_0 B_0}$;
3. for some B_0 -complete state $\omega_{A_0 B_0}$, with $\mathcal{H}_{B_0} \cong \mathcal{H}_{B'}$,
 $\rho_{AB} \otimes \omega_{A_0 B_0} \supseteq_{AA_0} \sigma_{AB'} \otimes \omega_{A_0 B_0}$.

Proof. We begin by noticing that the implication (1) \Rightarrow (2) is a trivial consequence of the fact that, if $\sigma_{AB'} = (\text{id}_A \otimes \mathcal{D}_B)(\rho_{AB})$ for some channel $\mathcal{D}_B : \mathbf{L}(\mathcal{H}_B) \rightarrow \mathbf{L}(\mathcal{H}_{B'})$, the action of any POVM $\{Q_{B'B_0}^x\}_x$ on $\sigma_{AB'} \otimes \omega_{A_0 B_0}$ can be exactly simulated on $\rho_{AB} \otimes \omega_{A_0 B_0}$ by using the POVM $\{(\mathcal{D}_{B'}^* \otimes \text{id}_{B_0})(Q_{B'B_0}^x)\}_x$, where we denoted by $\mathcal{D}_{B'}^* : \mathbf{L}(\mathcal{H}_{B'}) \rightarrow \mathbf{L}(\mathcal{H}_B)$ the Heisenberg dual of \mathcal{D}_B .

Also the implication (2) \Rightarrow (3) is trivial.

We are then left to prove that (3) \Rightarrow (1). In order to do so, we consider two auxiliary Hilbert spaces \mathcal{H}_{A_0} and \mathcal{H}_{B_0} , such that $\mathcal{H}_{B_0} \cong \mathcal{H}_{B'}$, and a B_0 -complete state $\omega_{A_0 B_0}$ (see Def. 10). We then consider, in particular, the following measurement on the composite state $\sigma_{AB'} \otimes \omega_{A_0 B_0}$:

$$\text{Tr}[(\Upsilon_A^y \otimes \Xi_{A_0}^x \otimes B_{B'B_0}^z) (\sigma_{AB'} \otimes \omega_{A_0 B_0})],$$

where

- $\{\Upsilon_A^y\}_y$ is an informationally complete POVM on \mathcal{H}_A (i.e. any operator in $\mathbf{L}(\mathcal{H}_A)$ can be written as a linear combination of its elements);
- $\{\Xi_{A_0}^x\}_x$ is the POVM on \mathcal{H}_{A_0} , whose existence is guaranteed by Lemma 1, inducing a complete set of linearly independent reduced (subnormalised) states $\omega_{B_0}^x = \text{Tr}_{A_0}[(\Xi_{A_0}^x \otimes \mathbb{1}_{B_0}) \omega_{A_0 B_0}]$ on \mathcal{H}_{B_0} ;
- $\{B_{B'B_0}^z\}_z$ is a generalised Bell measurement on $\mathcal{H}_{B'} \otimes \mathcal{H}_{B_0} \cong \mathcal{H}_{B'}^{\otimes 2}$ (i.e. a complete set of $(\dim \mathcal{H}_{B'})^2$ orthogonal maximally entangled states).

First of all, we know that, by Theorem 3 condition 3, there exists a POVM $\{R_{BB_0}^z\}_z$ such that

$$\text{Tr}[(\Upsilon_A^y \otimes \Xi_{A_0}^x \otimes R_{BB_0}^z) (\rho_{AB} \otimes \omega_{A_0 B_0})] = \text{Tr}[(\Upsilon_A^y \otimes \Xi_{A_0}^x \otimes B_{B'B_0}^z) (\sigma_{AB'} \otimes \omega_{A_0 B_0})],$$

for every triple (x, y, z) . Then, by first performing the trace over \mathcal{H}_{A_0} , we obtain the following identity:

$$\text{Tr}[(\Upsilon_A^y \otimes R_{BB_0}^z) (\rho_{AB} \otimes \omega_{B_0}^x)] = \text{Tr}[(\Upsilon_A^y \otimes B_{B'B_0}^z) (\sigma_{AB'} \otimes \omega_{B_0}^x)], \quad (15)$$

where, as we noticed above, $\text{span}\{\omega_{B_0}^x\} = \mathbf{L}(\mathcal{H}_{B_0})$.

We now introduce another Hilbert space $\mathcal{H}_{B_1} \cong \mathcal{H}_{B_0} \cong \mathcal{H}_{B'}$ and fix orthonormal bases $\{|\alpha^i\rangle\}_i$ and $\{|\beta^j\rangle\}_j$ for \mathcal{H}_{B_1} and \mathcal{H}_{B_0} , respectively. Further, let the standard maximally entangled state in $\mathcal{H}_{B_1} \otimes \mathcal{H}_{B_0}$ be given by

$$|\Phi_{B_1 B_0}^+\rangle := d^{-1/2} \sum_i |\alpha_{B_1}^i\rangle \otimes |\beta_{B_0}^i\rangle,$$

where $d := \dim \mathcal{H}_{B_1} = \dim \mathcal{H}_{B_0} = \dim \mathcal{H}_{B'}$. Let us, moreover, define the operators

$$\begin{aligned} \Omega_{B_1}^x &= d^2 \operatorname{Tr}_{B_0}[(\mathbb{1}_{B_1} \otimes \omega_{B_0}^x) |\Phi_{B_1 B_0}^+\rangle \langle \Phi_{B_1 B_0}^+|] \\ &= d (\omega_{B_1}^x)^T, \end{aligned}$$

where the transposition is made with respect to the basis chosen in the definition of $|\Phi_{B_1 B_0}^+\rangle$. Clearly, $\operatorname{span}\{\omega_{B_0}^x\} = \mathbf{L}(\mathcal{H}_{B_0})$ implies that $\operatorname{span}\{\Omega_{B_1}^x\} = \mathbf{L}(\mathcal{H}_{B_1})$, since neither the transposition nor the multiplication by a non-zero scalar affect the property of being linearly independent. It is moreover easy to verify (even by direct inspection) that

$$\operatorname{Tr}_{B_1}[(\Omega_{B_1}^x \otimes \mathbb{1}_{B_0}) |\Phi_{B_1 B_0}^+\rangle \langle \Phi_{B_1 B_0}^+|] = \omega_{B_0}^x$$

for all x .

Going back to Eq. (15), we can therefore rewrite it as:

$$\operatorname{Tr}[(\Upsilon_A^y \otimes \Omega_{B_1}^x \otimes R_{B B_0}^z) (\rho_{AB} \otimes |\Phi^+\rangle \langle \Phi^+|_{B_1 B_0})] = \operatorname{Tr}[(\Upsilon_A^y \otimes \Omega_{B_1}^x \otimes B_{B' B_0}^z) (\sigma_{AB'} \otimes |\Phi^+\rangle \langle \Phi^+|_{B_1 B_0})].$$

Since both $\{\Upsilon_A^y\}_y$ and $\{\Omega_{B_1}^x\}_x$ are a complete set of linearly independent operators [27], the above equality is, in fact, an operator identity:

$$\operatorname{Tr}_{B B_0}[(\mathbb{1}_{AB_1} \otimes R_{B B_0}^z) (\rho_{AB} \otimes |\Phi^+\rangle \langle \Phi^+|_{B_1 B_0})] = \operatorname{Tr}_{B' B_0}[(\mathbb{1}_{AB_1} \otimes B_{B' B_0}^z) (\sigma_{AB'} \otimes |\Phi^+\rangle \langle \Phi^+|_{B_1 B_0})], \quad (16)$$

for all z .

We recall now that the POVM $\{B_{B' B_0}^z\}_z$, appearing on the right-hand side of the above equation, has been chosen to constitute a generalised Bell measurement on $\mathcal{H}_{B'} \otimes \mathcal{H}_{B_0} \cong \mathcal{H}_{B'}^{\otimes 2}$. Therefore, the protocol of quantum teleportation provides unitary operators $U^z : \mathcal{H}_{B_1} \rightarrow \mathcal{H}_{B'}$ such that

$$\sum_z (\mathbb{1}_A \otimes U_{B_1}^z) \left\{ \operatorname{Tr}_{B' B_0}[(\mathbb{1}_A \otimes \mathbb{1}_{B_1} \otimes B_{B' B_0}^z) (\sigma_{AB'} \otimes |\Phi^+\rangle \langle \Phi^+|_{B_1 B_0})] \right\} (\mathbb{1}_A \otimes U_{B_1}^z)^\dagger = \sigma_{AB'}.$$

Then, by defining a CPTP map $\mathcal{D} : \mathbf{L}(\mathcal{H}_B) \rightarrow \mathbf{L}(\mathcal{H}_{B'})$:

$$\mathcal{D}(X_B) := \sum_z U_{B_1}^z \left\{ \operatorname{Tr}_{B B_0}[(\mathbb{1}_{B_1} \otimes R_{B B_0}^z) (X_B \otimes |\Phi^+\rangle \langle \Phi^+|_{B_1 B_0})] \right\} (U_{B_1}^z)^\dagger,$$

for all $X_B \in \mathbf{L}(\mathcal{H}_B)$, we arrive at

$$(\operatorname{id}_A \otimes \mathcal{D})(\rho_{AB}) = \sigma_{AB'},$$

i.e. $\rho_{AB} \succ \sigma_{AB'}$. ■

4 ...and back to channels

The starting observation is that, due to the invertibility of the Choi isomorphism (Theorem 2), a channel \mathcal{N} can be degraded to another channel \mathcal{M} (i.e. there exists a third channel \mathcal{D} such that $\mathcal{M} = \mathcal{D} \circ \mathcal{N}$) if and only if the bipartite state $\rho^\mathcal{N}$ can be locally degraded to $\rho^\mathcal{M}$, in the sense of Definition 9. However, before being able to translate Theorem 4 into its analogue for channels, we first have to understand what sort of channels induce complete (in the sense of Definition 10) Choi states. The answer is given by the following definition:

Definition 11 (Complete channels). *A channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ is said to be complete whenever its range contains $(\dim \mathcal{H}_B)^2$ linearly independent elements.*

Other than the trivial example of the identity channel, another, more interesting class of channels that are complete is given by d -dimensional symmetric channels of Definition 2.

Lemma 2. *A channel is complete if and only if its associated Choi state is complete, in the sense of Def. 10. In particular, all d -dimensional symmetric channels are complete together with their associated Choi states.*

Proof. Let $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ be a complete channel. By definition there exist $(\dim \mathcal{H}_B)^2$ input states ρ_A^i such that the set $\{\mathcal{N}(\rho_A^i) : 1 \leq i \leq (\dim \mathcal{H}_B)^2\}$ spans the whole $\mathbf{L}(\mathcal{H}_B)$.

We now recall the fact, sometimes referred to as *steering* [26], that, for any state ρ_A , there exists an operator $P_{\tilde{A}} > 0$ such that $\rho_A = \text{Tr}_{\tilde{A}}[(P_{\tilde{A}} \otimes \mathbb{1}_A) |\Phi_{\tilde{A}A}^+\rangle\langle\Phi_{\tilde{A}A}^+|]$, where $\mathcal{H}_{\tilde{A}} \cong \mathcal{H}_A$ and $|\Phi_{\tilde{A}A}^+\rangle$ is a maximally entangled state in $\mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_A$. Therefore, for any given channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$, its Choi state $\rho_{AB}^{\mathcal{N}}$ is constructed so that, for any input state ρ_A , there exists an operator $P_A > 0$ such that $\mathcal{N}(\rho_A) = \text{Tr}_A[(P_A \otimes \mathbb{1}_B) \rho_{AB}^{\mathcal{N}}]$. In turn, this implies that, whenever the channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$ is complete, there exists a set of operators $\{P_A^i > 0 : 1 \leq i \leq (\dim \mathcal{H}_B)^2\}$ such that the set $\{\text{Tr}_A[(P_A^i \otimes \mathbb{1}_B) \rho_{AB}^{\mathcal{N}}] : 1 \leq i \leq (\dim \mathcal{H}_B)^2\}$ spans the whole $\mathbf{L}(\mathcal{H}_B)$, i.e. the bipartite state $\rho_{AB}^{\mathcal{N}}$ is complete, according to Definition 10.

Conversely, suppose that the Choi state $\rho_{AB}^{\mathcal{N}}$, associated with a channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$, is (B) -complete, in the sense of Definition 10. Then, by definition, there exist $(\dim \mathcal{H}_B)^2$ operators $P_A^i > 0$ such that the states defined as $\rho_B^i := \text{Tr}_A[(P_A^i \otimes \mathbb{1}_B) \rho_{AB}^{\mathcal{N}}]$ are all linearly independent in $\mathbf{L}(\mathcal{H}_B)$. On the other hand, $\rho_B^i = \text{Tr}_A[(P_A^i \otimes \mathbb{1}_B) \rho_{AB}^{\mathcal{N}}] = \text{Tr}_{\tilde{A}}[(P_{\tilde{A}}^i \otimes \mathbb{1}_B) (\text{id}_{\tilde{A}} \otimes \mathcal{N}_A)(|\Phi_{\tilde{A}A}^+\rangle\langle\Phi_{\tilde{A}A}^+|)] = \mathcal{N}_A(\rho_A^i)$, where $\rho_A^i := \text{Tr}_{\tilde{A}}[(P_{\tilde{A}}^i \otimes \mathbb{1}_B) |\Phi_{\tilde{A}A}^+\rangle\langle\Phi_{\tilde{A}A}^+|]$, i.e., all ρ_B^i belong to the range of the channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$, meaning that \mathcal{N} is complete in the sense of Definition 11.

Let us now turn to the special case of d -dimensional symmetric channels, as introduced in Definition 2. We just show that the channels are complete; the completeness of the corresponding Choi states then comes automatically. Consider therefore any d -dimensional symmetric channel \mathcal{S} , defined by two d -dimensional Hilbert spaces \mathcal{H}_B and $\mathcal{H}_E \cong \mathcal{H}_B$, a $\frac{d(d+1)}{2}$ -dimensional Hilbert space \mathcal{H}_A , and an isometry $V : \mathcal{H}_A \rightarrow (\mathcal{H}_B \otimes \mathcal{H}_E)_{\text{sym}}$. Choose now $(\dim \mathcal{H}_B)^2$ vectors $\{|\phi_B^i\rangle\}$ in \mathcal{H}_B such that the corresponding rank-one states $|\phi_B^i\rangle\langle\phi_B^i|$ are all linearly independent in $\mathbf{L}(\mathcal{H}_B)$. Since $|\phi_B^i\rangle \otimes |\phi_E^i\rangle \in (\mathcal{H}_B \otimes \mathcal{H}_E)_{\text{sym}}$ for all i , all the $(\dim \mathcal{H}_B)^2$ pure states $\text{Tr}_E[|\phi_B^i\rangle\langle\phi_B^i| \otimes |\phi_E^i\rangle\langle\phi_E^i|] = |\phi_B^i\rangle\langle\phi_B^i|$ are possible outputs of \mathcal{S} , i.e., \mathcal{S} is complete. Therefore, its associated Choi state $\omega_{AB}^{\mathcal{S}} := (\text{id} \otimes \mathcal{S})(|\Phi^+\rangle\langle\Phi^+|) = \text{Tr}_E[(\mathbb{1} \otimes V)(|\Phi^+\rangle\langle\Phi^+|)(\mathbb{1} \otimes V^\dagger)]$ is a complete state. \blacksquare

We are now ready to prove Theorem 1. In fact, we will do this indirectly, by proving that Theorem 1 is nothing but Theorem 4 formulated for a channel, rather than for a bipartite quantum state.

Proof of Theorem 1. Since implications (1) \Rightarrow (2), and (2) \Rightarrow (3) are trivial, we will focus only on the implication (3) \Rightarrow (1).

In order to prove the implication (3) \Rightarrow (1), first of all we notice that, given two channels $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_\alpha)$ and $(\mathcal{H}_A, \mathcal{H}_{B'}, \mathcal{N}_{\beta'})$, the Choi isomorphism (Theorem 2) provides two bipartite states $\rho_{AB}^\alpha := (\text{id} \otimes \mathcal{N}^\alpha)(|\Phi^+\rangle\langle\Phi^+|)$ and $\sigma_{AB'}^\beta := (\text{id} \otimes \mathcal{N}^\beta)(|\Phi^+\rangle\langle\Phi^+|)$ such that $\text{Tr}_B \rho_{AB}^\alpha = \text{Tr}_{B'} \sigma_{AB'}^\beta = d_A^{-1} \mathbb{1}_A$. We can therefore apply Theorem 4 to ρ_{AB}^α and $\sigma_{AB'}^\beta$.

Since point (3) of Theorem 4 requires the comparison to be performed with some additional complete bipartite state, we can take the state $\omega_{A_0 B_0}$ appearing in point (3) of Theorem 4 to be, in fact, the Choi state corresponding to a d_{B_0} -symmetric channel, which we know it is complete as a consequence of Lemma 2.

We then notice that, playing a ‘static’ guessing game, as defined in Eq. (5), with some Choi state is statistically equivalent to playing a ‘dynamic’ guessing game with the corresponding channel, as described in Definition 4. The relation between the two approaches is again given by steering. As already noticed in the proof of Lemma 2, for any given channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N})$, its Choi state $\rho_{AB}^{\mathcal{N}}$ is constructed so that, for any ensemble $(\mathcal{H}_A, \mathcal{X}, \{p_x, \rho_A^x\})$ there exists a POVM $\{P_A^x\}$ such that $p_x \mathcal{N}(\rho_A^x) = \text{Tr}_A[(P_A^x \otimes \mathbb{1}_B) \rho_{AB}^{\mathcal{N}}]$ for all x .

It is therefore clear that point (3) in Theorem 4 is completely equivalent (in fact, just a reformulation) of point (3) in Theorem 1. Since point (3) in Theorem 4 is also equivalent to point (1) in Theorem 4, we are left to show that point (1) in Theorem 4 is just a reformulation of point (1) in Theorem 1. The logical steps are summarized as follows:

$$\text{Thm. 1, point (3)} \quad \Leftrightarrow \quad \text{Thm. 4, point (3)} \quad \Leftrightarrow \quad \text{Thm. 4, point (1)} \quad \Leftrightarrow \quad \text{Thm. 1, point (1)},$$

where the first equivalence has been proved above, the second equivalence is in the statement of Theorem 4, and only the last equivalence is left to be proved. But this is a simple consequence of the fact that Choi's correspondence is one-to-one, therefore two channels \mathcal{N}_α and \mathcal{N}_β are such that there exists a third channel \mathcal{D} with $\mathcal{N}_\beta = \mathcal{D} \circ \mathcal{N}_\alpha$, if and only if $\rho_{AB}^{\mathcal{N}_\alpha} \succ \rho_{AB}^{\mathcal{N}_\beta}$. ■

5 Further implications of Theorem 1

One can extend the results of Theorem 1 to convex combinations of channels. It was shown in [25] that degradable channels and degradable extensions have especially nice properties which prove to be useful when evaluating their quantum and private capacities. These properties are also reflected in the game-theoretic framework. In particular, the following two corollaries show how to compare and combine convex combinations of degradable channels and their extensions in this framework.

Corollary 2. *Consider a channel $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_\beta)$, and a sequence of channels $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_i)$, $i = 1, \dots, n$, such that $\mathcal{N}_\beta = \sum_i p_i \mathcal{N}_i$. Assume that each \mathcal{N}_i is degradable, with the corresponding degrading map is given by $(\mathcal{H}_B, \mathcal{H}'_B, \mathcal{D}_i)$. Define the flagged version of the convex combination of \mathcal{N}_i as $\mathcal{T} = \sum_i p_i \mathcal{N}_i \otimes |i\rangle\langle i|$. Then, \mathcal{T} is strongly more informative than \mathcal{N}_β , i.e. $\mathcal{T} \supseteq_s \mathcal{N}_\beta$.*

Proof. It was proven in [25] that \mathcal{T} is a degradable extension of \mathcal{N}_β . Then the corollary follows after applying Theorem 1. ■

Corollary 3. *Consider two channels $(\mathcal{H}_A, \mathcal{H}_B, \mathcal{N}_i)$, $i = 1, 2$, for each of which there exist $(\mathcal{H}_A, \mathcal{H}'_B, \mathcal{T}_i)$ and $(\mathcal{H}'_B, \mathcal{H}_B, \mathcal{D}_i)$ such that $\mathcal{N}_i = \mathcal{D}_i \circ \mathcal{T}_i$ for $i = 1, 2$. Then, for $\mathcal{T} = p\mathcal{T}_1 \otimes |1\rangle\langle 1| + (1-p)\mathcal{T}_2 \otimes |2\rangle\langle 2|$ and $\mathcal{N} = p\mathcal{N}_1 + (1-p)\mathcal{N}_2$ we have that \mathcal{T} is strongly more informative than \mathcal{N} : $\mathcal{T} \supseteq_s \mathcal{N}$.*

Proof. It is sufficient to observe that \mathcal{T} is a degradable extension of \mathcal{N} [25]. Then the corollary follows after applying Theorem 1. ■

6 Conclusions

We introduced a game-theoretic framework 1.1 which allowed us to derive a necessary and sufficient condition for a channel to be antidegradable. We showed that for any channel which is not antidegradable, there exists an encoding strategy for which such a channel provides a strict advantage for the two players over the adversary in the guessing game that we defined. The key ingredients in the proof of this result are the tools of statistical comparison of bipartite quantum states, and the Choi isomorphism.

The exact relationship between our game-theoretic framework and the standard information-theoretic framework remains to be explored. It would be interesting to see whether any inference about the quantum or private capacity of a quantum channel could be made from results obtained in our game-theoretic framework.

Another direction worth pursuing is one which involves devising game-theoretic characterizations of other classes of quantum channels, since this might lead to a better understanding of the structure of zero-capacity channels. It would also be interesting to explore the connections between our game-theoretic approach and other incapacity tests [9] for quantum channels.

Acknowledgements

The authors are grateful to Michele Dall'Arno for suggesting an improvement to their previous proof of Lemma 1. S.S. acknowledges the support of Sidney Sussex College.

References

- [1] I. Devetak, *The private classical capacity and quantum capacity of a quantum channel*. IEEE Transactions on Information Theory **51**, Issue 1, pp 44-55 (January 2005).

- [2] When the viceversa is true, i.e., when a post-processing of the channel's output can simulate the output to the environment, we speak of *degradable channels* [3, 4].
- [3] I. Devetak and P. W. Shor, *The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information*. Communications in Mathematical Physics **256**, Issue 2, pp 287-303 (June 2005).
- [4] T. S. Cubitt, M.-B. Ruskai, and G. Smith, *The structure of degradable quantum channels*. J. Math. Phys. **49**, 102104 (2008).
- [5] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, , Published online: 28 October 1982; | doi:10.1038/299802a0, 299 (1982), pp. 802–803.
- [6] P. Horodecki, M. Horodecki, and R. Horodecki, *Binding entanglement channels*, quant-ph/9904092, (1999). J.Mod.Opt. 47 (2000) 347-354.
- [7] K. Li, A. Winter, X. Zou, and G. Guo, *Private capacity of quantum channels is not additive*, Physical Review Letters, 103 (2009), p. 120501.
- [8] G. Smith and J. A. Smolin, *Extensive nonadditivity of privacy*, Physical Review Letters, 103 (2009), p. 120503.
- [9] G. Smith and J. A. Smolin, *Detecting incapacity of a quantum channel*, Physical Review Letters, 108 (2012), p. 230507.
- [10] F. G. S. L. Brandão, J. Oppenheim, and S. Strelchuk, *When does noise increase the quantum capacity?*, Phys. Rev. Lett., 108 (2012), p. 040501.
- [11] G. Smith, J. A. Smolin, and J. Yard, *Quantum communication with gaussian channels of zero quantum capacity*, Nature Photonics, 5 (2011), pp. 624–627.
- [12] G. Smith and J. Yard, *Quantum communication with zero-capacity channels*, Science, 321 (2008), pp. 1812–1815.
- [13] W. F. Stinespring, *Positive functions on C^* -algebras*, Proc. Amer. Math. Soc., 6 (1955), pp. 211–216.
- [14] A. S. Holevo, *On complementary channels and the additivity problem*. Probab. Theory and Appl. **51**, 133-143 (2005).
- [15] E Shmaya, *Comparison of information structures and completely positive maps*. J. Phys. A: Math. and Gen. **38**, 9717-9727 (2005).
- [16] A Cheffles, *The Quantum Blackwell Theorem and Minimum Error State Discrimination*. ArXiv:0907.0866v4 [quant-ph].
- [17] M-D Choi, *Positive linear maps on C^* -algebras*. Canad. J. Math. **24**, 520-529 (1972).
- [18] G M D'Ariano and P Lo Presti, *Imprinting a complete information about a quantum channel on its output state*. Phys. Rev. Lett. **91**, 047902 (2003).
- [19] F Buscemi, *Comparison of Quantum Statistical Models: Equivalent Conditions for Sufficiency*. Comm. Math. Phys. **310**, 625–647 (2012).
- [20] F Buscemi, *All Entangled States are Nonlocal*. Phys. Rev. Lett. **108**, 200401 (2012).
- [21] G Smith, J A Smolin, and A Winter, *The quantum capacity with symmetric side channels*. IEEE Trans. Info. Theory **54**, 9, 4208-4217 (2008).
- [22] F G S L Brandão and J Oppenheim, *The quantum one-time pad in the presence of an eavesdropper*. Phys. Rev. Lett. **108**, 040504 (2012).
- [23] F G S L Brandão and J Oppenheim, *Public Quantum Communication and Superactivation*. IEEE Trans. Info. Theo. **59**, 2517 (2013).

- [24] Note, however, that there exist channels which convey the same information to both Bob and Eve, but which cannot be written as d -dimensional symmetric channels. An example is given by the 50% erasure channel mentioned in the introduction, which maps d -dimensional inputs into $(d + 1)$ -dimensional outputs.
- [25] Graeme Smith, John A. Smolin, *Additive Extensions of a Quantum Channel*. Proc. of the IEEE Inf. Th. Workshop 2008, pp 368-372.
- [26] E. Schrodinger, Proc. Camb. Phil. Soc. **31**, 555 (1935).
- [27] In fact, while $\{\Upsilon_A^y\}_y$ is, in particular, a POVM, $\{\Omega_{B_1}^x\}_x$ in general is not, since $\sum_x \Omega^x \neq 1$. Nonetheless, they are both complete spanning sets for $\mathbf{L}(\mathcal{H}_A)$ and $\mathbf{L}(\mathcal{H}_{B_1})$, respectively.